Rückblick auf die DZSF-Fachkonferenz Cybersecurity-Forschung

Cybersecurity ist auch im Schienenverkehr von großer Bedeutung. Das DZSF stellte erste Forschungsergebnisse vor und wirbt für eine Zusammenarbeit des Sektors.

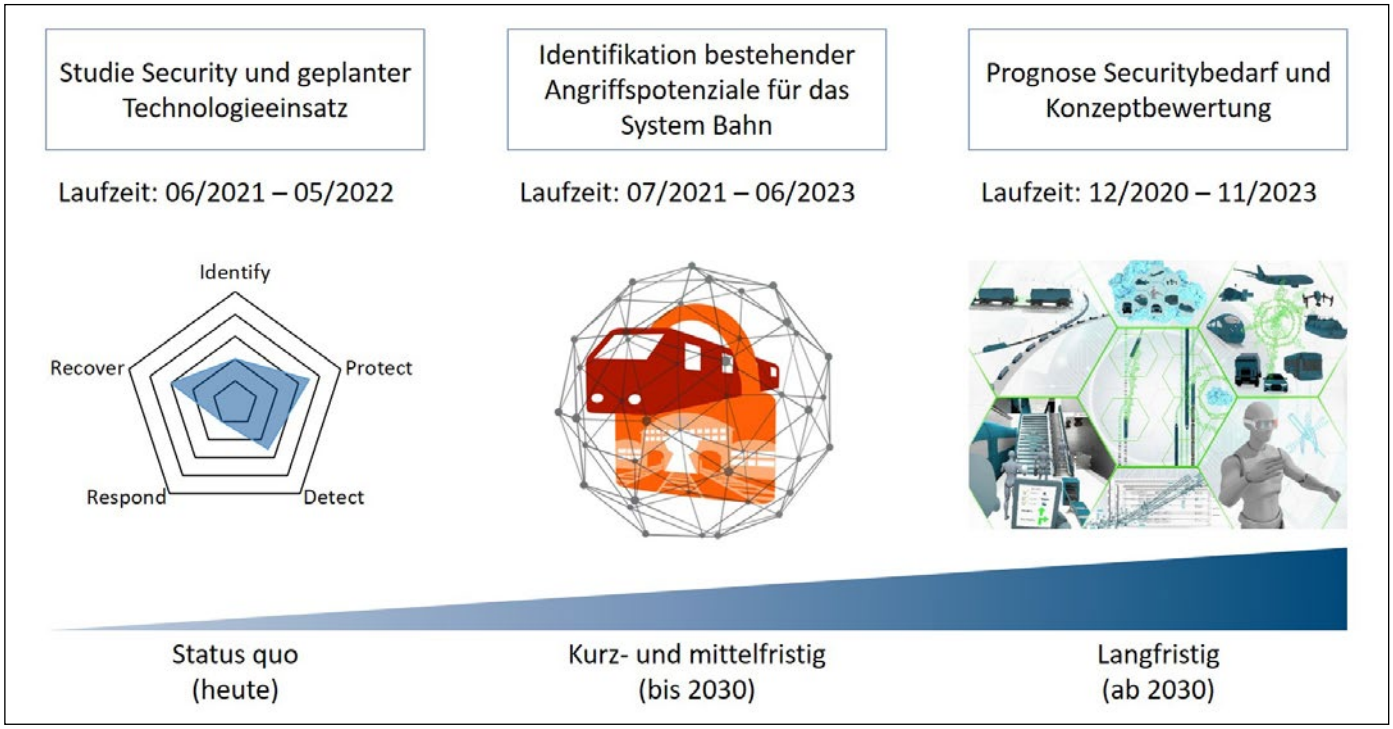

Abb. 1: Übersicht über die vorgestellten Cybersecurity-Projekte des DZSF

KRISTIN MÜHL | MARTIN LEHNERT | LUKAS IFFLÄNDER

Sichere Mobilität kann bei zunehmender Digitalisierung und verstärktem Einsatz von vernetzten Softwareanwendungen nur durch umfangreiche Cybersecurity-Maßnahmen gewährleistet werden. Für das Deutsche Zentrum für Schienenverkehrsforschung (DZSF) ist daher das Thema Cybersecurity im Schienenverkehr eines der priorisierten Forschungsthemen. Erste Ergebnisse der durch das DZSF initiierten und koordinierten Analysen und Forschungsprojekte wurden am 13. Oktober 2022 auf der online veranstalteten Fachkonferenz Cybersecurity-Forschung vorgestellt und im Rahmen einer Expertendiskussion vertieft.

Thematische Einführung

Cybersecurity ist im Zeitalter der Digitalisierung und stetigen Vernetzung der bereits eingesetzten und erprobten sowie neuen und aufstrebenden Technologien und Anwendungen eine essenzielle Voraussetzung für den sicheren Betrieb der Eisenbahn. Die Vulnerabilität dieser kritischen Infrastruktur wurde bereits durch verschiedene Cyber- und physische Angriffe, wie beispielsweise kürzlich durch die Sabotage der Telekommunikationsinfrastruktur der Deutschen Bahn AG (DB), verdeutlicht. Damit das System Bahn vor schwerwiegenderen Cyberangriffen bestmöglich geschützt werden kann, müssen alle Akteure im Schienenverkehr ein hohes Bewusstsein für Cybersecurity aufbauen und strategisch zielführend agieren. Diesen Prozess unterstützt das DZSF, indem es aktuelle und praxisnahe Forschungsthemen ableitet und bearbeitet sowie dem Sektor und der Öffentlichkeit entsprechende Ergebnisse zugänglich macht. Außerdem bietet das DZSF eine Plattform für die Vernetzung und den Fachaustausch der Beteiligten im Sektor, denn nur gemeinsam kann die Cybersecurity im System Bahn optimiert werden.

Im Sinne dieses Fachaustauschs bot die digital durchgeführte Fachkonferenz Cyber-security-Forschung am 13. Oktober 2022 den interessierten Vertretern aus Politik, Wissenschaft, Industrie sowie Aufsichts- und Zulassungsstellen die Möglichkeit, sich über aktuelle Forschungsergebnisse der vom DZSF in Auftrag gegebenen Cybersecurity-Projekte zu informieren und diese zu diskutieren.

Cybersecurity-Projekte am DZSF

Die Direktorin des DZSF, **Prof. Dr. Corinna Salander**, eröffnete die Fachkonferenz, nahm Bezug auf die aktuellen physischen Angriffe auf die Infrastruktur im Bahnsektor, zeigte die Notwendigkeit der Forschung zur Cybersecurity auf und stellte die Querbeziehungen zu weiteren Forschungsarbeiten im Zentrum her. Anschließend stellten die Auftragnehmer der drei durch das DZSF koordinierten Projekte zur Cybersecurity im Schienenverkehr die Ergebnisse ihrer aktuellen Untersuchungen vor. Diese Projekte decken mit ihrem jeweiligen Fokus verschiedene Zeitdimensionen ab – vom aktuellen Stand der Cybersecurity über kurz- und mittelfristige Maßnahmen zur Stärkung bis hin zu langfristigen Prognosemöglichkeiten der Cyber-security (Abb. 1).

Ergebnisse des Projekts „Security und geplanter Technologieeinsatz" [1] stellte **Prof. Dr. Dietmar Möller**, Technische Universität Clausthal,

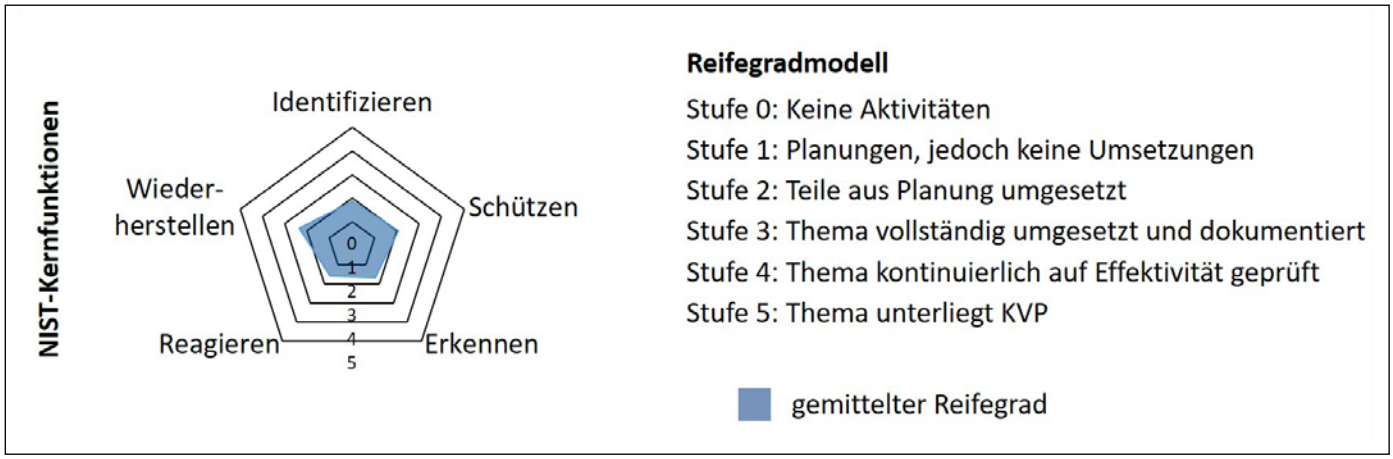

Abb. 2: Gesamtreifegrad der Cybersecurity über alle befragten Unternehmen, N=60 *Quelle: adaptiert nach IABG mbH*

vor. Neben der Erfassung des aktuellen Standes der Cybersecurity im Schienenverkehrssektor in Deutschland zielte das Projekt auch auf die Identifikation relevanter neuer Technologien und deren Securitybedarf ab. Dafür erfolgte eine zweistufige quantitative und qualitative Erhebung im Sektor mittels standardisiertem Fragebogen und vertiefenden Interviews. Dabei wurden die Reifegrade bezugnehmend auf die Cyber-security-Kernfunktionen des amerikanischen National Institute of Standards and Technology (NIST) [2] (Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen) von Unternehmen im Schienenverkehr erfasst. Die Untersuchung zeigt, dass zwar alle Unternehmen Cybersecurity-Maßnahmen umgesetzt haben, dies aber in sehr unterschiedlichen Ausprägungen. Im Mittel ist ein eher geringer Reifegrad der Cybersecurity zu verzeichnen, d. h. es wurden nur Teile aus der Planung umgesetzt (Abb. 2). Mit steigender Unternehmensgröße erhöht sich im Schnitt auch der Reifegrad [3, 4]. Insbesondere gilt es daher, kleine und mittelständige Unternehmen im Prozess der Optimierung der Cyber-security zu unterstützen.

Das Projekt „Identifikation bestehender Angriffspotenziale" zielt auf die ganzheitliche Identifikation der aktuellen Vulnerabilität des Systems Bahn ab und läuft noch bis Mitte des Jahres 2023 [5]. **Prof. Dr. Stefan Pickl**, Bundeswehr Universität München, führte aus, dass im Projekt die Schwachstellen in Bezug auf Cybersecurity, Organisation, Sprach- und Datenkommunikation sowie physische Eingriffe aufgezeigt und analysiert werden. Im bereits abgeschlossenen ersten Arbeitspaket des Projekts wurden die Angriffspotenziale systematisiert. Dazu wurden Vignetten aus den drei Aspekten Angriffsmittel, Angriffspunkt und Tätertyp gebildet. Alle drei Aspekte wurden detailliert untersetzt, wodurch insgesamt 868 Vignetten für Cyberangriffe entstanden. Anschließend wurden einige beispielhafte Vignetten ausgewählt und daraus unter Berücksichtigung von Ursachen und Folgen entsprechende Angriffsszenarien entwickelt. Eine fundierte Bewertung dieser Szenarien stellt die Voraussetzung zur Ableitung von Empfehlungen für Absicherungs- und Gegenstrategien zur Vorfallsbewältigung sowie zur Entwicklung von Präventionsmaßnahmen dar. Dieser Schritt folgt im weiteren Projektablauf.

Im Projekt „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn" wird eine proaktive Strategie zur Identifikation von Angriffsvektoren entwickelt. So kann nicht nur auf Angriffe reagiert

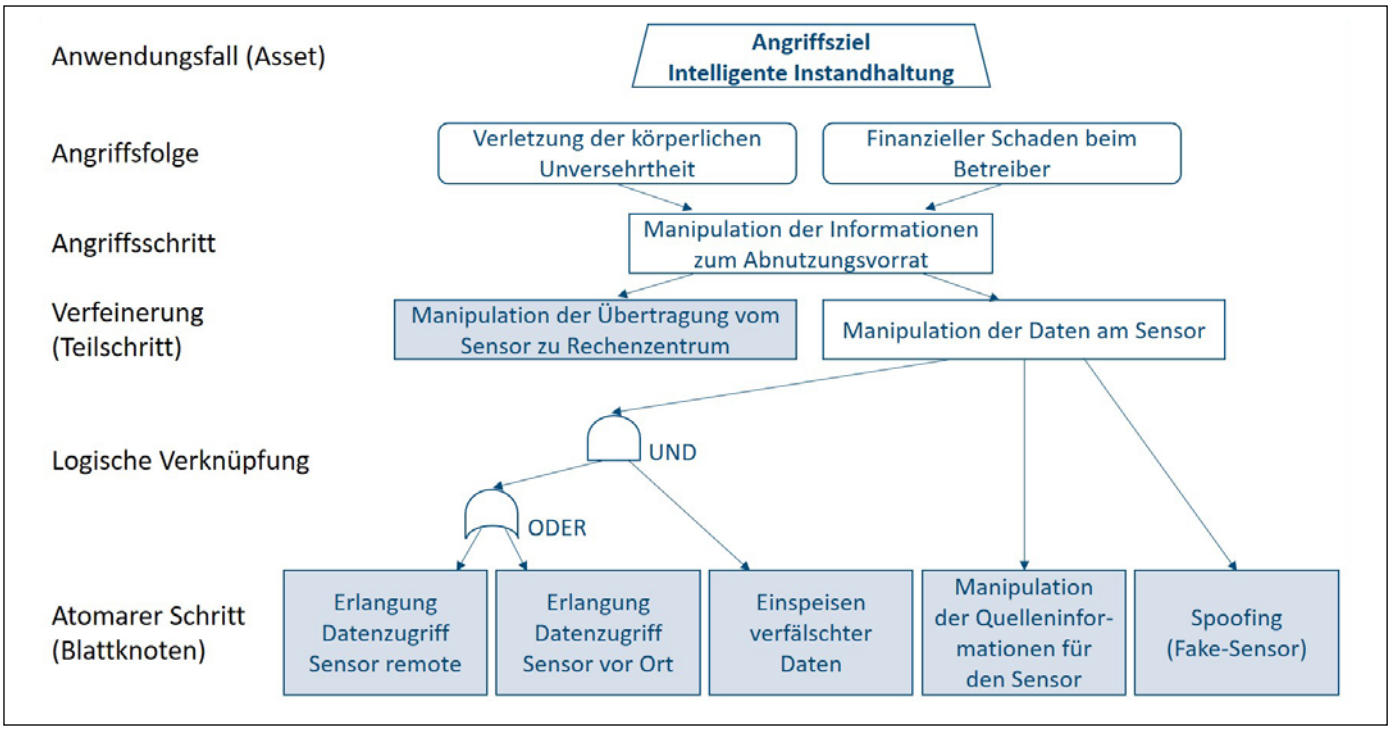

Abb. 3: Beispiel für einen Angriffsgraphen *Quelle: adaptiert nach Incyde GmbH*

werden, sie sind auch antizipierbar [6]. **Dr. Markus Heinrich**, Incyde GmbH Berlin, stellte die dafür im Rahmen des Projekts entwickelte softwaregestützte Bedrohungsanalyse durch Angriffsgraphen vor. Die frei verfügbare Software [7] sammelt für jeden betrachteten Anwendungsfall die möglichen Abuse-Cases (Missbrauchsfälle) im Angriffsgraphen und stellt damit den Zusammenhang von Angriff und Folge dar (Abb. 3). Eine granulare, logisch verknüpfte Verfeinerung in einzelne atomare Schritte (Blattknoten) ist damit möglich. Die Bewertung der Blattknoten wird damit gegenüber generischen Bedrohungen vereinfacht und präziser. Das Softwarewerkzeug unterstützt dann die Aggregation der Attribute bis zur Ableitung des Risikos [8]. Weiterhin stellte Herr Heinrich dar, wie dieses Verfahren und das Werkzeug auf die in einer Technologieprognose [9] ermittelten 21 Anwendungsfälle angewendet werden kann und aus welchen Bedrohungen sich typischerweise die höchsten Risiken ergeben [10]. Die Bewertung von effektiven und effizienten Schutzkonzepten und entsprechende Empfehlungen für das System Bahn zur Setzung von neuen Sicherheitsstandards sind die nächsten Schritte in diesem Forschungsprojekt.

i

Weiterführende Informationen
Die gezeigten Präsentationen der Veranstaltung finden Sie hier:

Expertendiskussion zum Thema Cybersecurity

Im zweiten Teil der Fachkonferenz des DZSF diskutierten Experten aus Wissenschaft, Industrie sowie Eisenbahnaufsicht und -zulassung in einem virtuellen Podium entscheidende Themenschwerpunkte im Kontext der Cybersecurity im Schienenverkehr und weiteren Forschungsbedarf.

Dr. Saeid Arabestani, Eisenbahn-Bundesamt, Leiter der Fachstelle IT-Sicherheit, hob hervor, dass die Sensibilität für Cybersecurity ebenso groß sein müsse wie für Safety-Fragestellungen. Um das Thema langfristig und nachhaltig im Sektor zu verankern, müsse sich eine Sicherheitskultur mit dem Fokus auf Cybersecurity entwickeln. Ferner sei die Frage, was sicherheitsrelevante Anwendungen sind, neu zu stellen. Beispielsweise könne ein manipulierter Anzeiger im Bahnhof auch Fahrgäste so lenken, dass er ein gefährliches Verhalten provoziert, welches schließlich Sicherheitsprobleme hervorruft. Die Industrie und der Betrieb werden gebraucht, damit die Erkenntnisse der Forschung beim Thema Cybersecurity in stärkerem Maß in den realen Betrieb einfließen könne.

Christian Paulsen, Siemens Mobility GmbH Braunschweig, ging darauf ein, dass Bedrohungsanalysen im Zusammenhang mit Software-Anwendungen und Kommunikationssystemen in der Leit- und Sicherungstechnik (LST) der Bahn bereits seit über zehn Jahren durchgeführt werden. Es bestehen Systeme, beispielsweise in einem Projekt in Norwegen, die bahnfeste Anwendungen mit einer entsprechenden Sicherheitsanforderungsstufe für die LST-Kommunikation über IP-Netze realisieren. Wichtig sei in diesem Zusammenhang aber auch, dass nicht nur in einzelnen Leuchtturmprojekten für neue Systeme die Cybersecurity untersucht und sichergestellt werde, sondern dass die Anwendung in der Fläche für alle Systeme erfolge. Dr. Arabestani ergänzte, dass auch die bestehenden Systeme hinsichtlich der Cybersecurity betrachtet und konsequent ertüchtigt werden müssten.

Prof. Dr. Stefan Katzenbeisser, Universität Passau, machte deutlich, dass die Aufrechterhaltung einer dauerhaften IT-Sicherheit eine Herausforderung darstelle. Dies sei schon darin begründet, dass die Cybersicherheit nicht einmalig bei Projektierung und Errichtung des Systems für alle Zeit nachgewiesen werden könne. Auch stochastische Betrachtungen seien bei Securitythemen nicht möglich. Vielmehr müsse die Cybersecurity als fortwährender Prozess verstanden werden, der dafür sorge, dass das System immer in einem guten, „securitysicheren" Zustand gehalten werde. Dazu gehöre neben der Redundanz der Systeme auch ein resilienter Aufbau sowohl gegen Cyberangriffe als auch physische und hybride Angriffe.

Prof. Dr. Stefan Pickl stellte heraus, dass Safety und Security nicht mehr getrennt betrachtet werden dürfen und die Verbindung beider Themen miteinander entscheidend sei. Mit Blick auf andere Branchen mit sicherheitskritischen Anwendungen (hier als Beispiel das Finanzwesen mit ca. 1/3 der Mitarbeitenden im IT-Bereich und davon wiederum 1/3 mit Fokus auf Cybersecurity-Fragen) sei im europäischen Bahnsektor zwar ein Bewusstsein vorhanden, jedoch viel zu wenig Personal verfügbar. Der Aufbau entsprechenden Personals sei eine dringende Aufgabe.

Zusammenfassung und Ausblick

Mit der Veranstaltung sind die große Relevanz des Themas Cybersecurity heute und in Zukunft sowie auch die Bandbreite an Themen im Kontext der Cybersecurity, mit denen sich das DZSF beschäftigt, ersichtlich geworden. Die drei vorgestellten Projekte weisen eine ganzheitliche Betrachtung auf, von der historischen Entwicklung von Cybersecurity und Angriffen über den Status quo des Cybersecurity-Bewusstseins, die bestehenden Angriffspotenziale, den zukünftigen Einsatz neuer Technologien bis hin zu kurz- und mittelfristig realisierbaren Schutzmaßnahmen und langfristigen Prognosemöglichkeiten von Angriffsvektoren im Schienenverkehr.

Insgesamt lässt sich aus den Studien ableiten, dass bezüglich der Cybersecurity bei vielen Unternehmen im Schienenverkehrssektor noch erheblicher Verbesserungsbedarf besteht. Insbesondere das Bewusstsein für Cybersecurity, aber auch die diesbezügliche Expertise müssen verstärkt werden. Cybersecurity muss als Prozess und nicht als Einmalmaßnahme verstanden werden. Es herrschte Einigkeit, dass das Thema Cybersecurity im Sektor eines gemeinsamen Vorgehens und eines Zusammenwirkens der Akteure aus Industrie, Wissenschaft sowie Eisenbahnaufsicht und -zulassung bedarf.

Das DZSF wird hierbei auch weiterhin den gezielten Austausch forcieren, das Wissen zur Cybersecurity und praxisrelevante Maßnahmen auf Basis wissenschaftlicher Erkenntnisse im Sektor verbreiten und den Entwicklungsprozess im deutschen Schienenverkehrssektor langfristig begleiten. Dabei werden zukünftig zusätzlich zu den umfangreichen theoretischen Analysen auch praktische Untersuchungen im eigenen Cybersecurity-Labor erfolgen. ■

QUELLEN

[1] Deutsches Zentrum für Schienenverkehrsforschung (2021): Projektwebseite „Security und geplanter Technologieeinsatz." Online unter: https://www.dzsf.bund.de/SharedDocs/Standardartikel/DZSF/Projekte/Projekt_86_Security_Technologieeinsatz.html, letzter Abruf am 25.10.2022 um 20:11 Uhr

[2] National Institute of Standards and Technology (2018): „Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1", National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, doi: 10.6028/NIST.CSWP.04162018

[3] Iffländer, L.; Mühl, K.; Nord, M.: „Sind Eisenbahn- und ÖPNV-Sektor fit für die heutigen Cybersecurity-Herausforderungen?" ETR – Eisenbahntechnische Rundschau (71), 11/2022, S. 10-15

[4] Möller, D.; Iffländer, L.; Nord, M.; Leppla, B.; Krause, P.; Czerkewski, P.; Lenski, N.; Mühl, K.: "Cybersecurity in the German Railway Sector". Proceedings of the 17th International Conference on Critical Information Infrastructure Security (CRITIS 2022), 14.-16. September 2022, München

[5] Deutsches Zentrum für Schienenverkehrsforschung (2022): Projektwebseite „Cybersecurity – Identifikation bestehender Angriffspotentiale". Online unter: https://www.dzsf.bund.de/SharedDocs/Standardartikel/DZSF/Projekte/Projekt_61_Cybersecurity.html, letzter Abruf am 25.10.2022 um 21:43 Uhr

[6] Deutsches Zentrum für Schienenverkehrsforschung (2020): Projektwebseite „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn". Online unter: https://www.dzsf.bund.de/SharedDocs/Standardartikel/DZSF/Projekte/Projekt_49_Securitybedarf.html, letzter Abruf am 25.10.2022 um 22:06 Uhr

[7] Incyde GmbH: Software Repository zum Projekt (2022): „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn". Online unter: https://github.com/INCYDE-GmbH/attackgraphs, letzter Abruf am 25.10.2022 um 22:26 Uhr

[8] Heinrich, M.; Iffländer, L.: „Softwaregestützte Bedrohungsanalyse durch Angriffsgraphen", SIGNAL+DRAHT (114), 05/2022, S. 28-34

[9] Leining, M.; Schubert, M.; Heinrich, M.; Katzenbeisser, S.; Unger, S.; Krauß, C.; Scheuermann, D. (2022): „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte – Teil 1: Technologieprognose". Deutsches Zentrum für Schienenverkehrsforschung (Hrsg.), Berichte des Deutschen Zentrums für Schienenverkehrsforschung 20, doi: 10.48755/dzsf.220008.06

[10] Heinrich, M.; Iffländer, L.; Scheuermann, D.; Katzenbeisser, S.; Unger, S.: „Technologie- und Securityprognose System Bahn – Bedrohungen rechtzeitig erkennen", SIGNAL+DRAHT (114), 09/2022, S. 96-103

Dr. Kristin Mühl
Wissenschaftliche Referentin
Human Factors
muehlk@dzsf.bund.de

Prof. Dr. Martin Lehnert
Forschungsbereichsleiter Sicherheit
lehnertm@dzsf.bund.de

Dr. Lukas Iffländer
Wissenschaftlicher Referent
Cybersecurity
ifflaenderl@dzsf.bund.de

Alle Autoren:
Deutsches Zentrum für Schienenverkehrsforschung (DZSF), Dresden

Rail Bücher & Reports

GEBÜNDELTES WISSEN – ÜBERSICHTLICH UND AKTUELL

www.eurailpress.de/fachbuecher-reports

Jetzt bestellen!

DVV Media Group

Eurail press